FORMAN CHRISTIAN COLLEGE (A Chartered University)
Course Outline and Lesson Plan

Spring 2023 Semester

Course Name: Information Security

Course Code: Comp 421	**Course Type :** Major / Compulsory	**Course Credits:** Three (3) Credit Hours
Class Timings: 2:00 pm to 2:50 pm on MWF	**Section:** A	**Student Meeting Hours/ Office Hours:** 04:00 pm to 05:00 pm on MW 04:00 pm to 04:45 pm on F

Instructor Name: Dr. Saad Bin Saleem

A note from the Instructor: The **learning** model for this course is face to face (in person). However, the instructor can **adop**t either an on-line or blended learning model according to the **instructions** by the **university administration** in any **special circumstances**.

In the **face-to-face learning model**, the instructor would **conduct live lectures / presentations** in the **assigned classroom** in front of the **students**.
Other than **following** the live lectures, you are **expected** to **regularly check** the **Moodle announcements** and follow the **course's weekly plan** given in this **course outline**. You are expected to do **weekly tasks** by **reading** the **shared material** e.g. lecture slides, book chapters and video tutorials, reading / preparing the assigned tasks e.g. quizzes and assignments. All the **reading material** and **assigned work** for assessment will be available under **weekly activity or resource** link on the **Moodle**.

Teaching Philosophy: As a passionate practitioner and research in the field of information security, I am committed to your learning. However, I also expect from you to focus on achieving grades through learning rather using unfair means like plagiarism and copy.

Instructor Contact Details:
Email: saadsaleem@fccollege.edu.pk

Office Hours: (face to face and/ or online): 04:00 pm to 05:00 pm.

Guidelines for contacting instructor: For a face to face meeting, you can walk into my office by knocking the door during my office hours. For an online meeting, I will remain online on zoom during my office hours. You can send a request using the Zoom meeting link to join the meeting.
In case of any meeting other than office hours, you are required to book the meeting well-before time through an email. Normally, I try my best to **respond** to any **email** by my students **within** the **twenty four (24) hours.** Therefore, you **do not need** to **resend** the **same email within** the **twenty fours (24 hours).** I encourage students to **contact during** the **day-time** from **09:00 am to 05:00 pm. Please do not expect a reply of email during the holidays e.g. weekends and after 06:00** pm. Any meeting outside of office hours should be booked through my official email ***saadsaleem@fccollege.edu.pk***.

TA Name and Contact Details:
Name: To be decided.
Email:
Office Hours: N/A
Guidelines for contacting TA/s: You can contact the course TA through email, phone or meet him in person.

Course Description: To provide the knowledge of basic concepts relevant to the field of information security. The students will also get essential training to practically apply the learned concepts. The students will be able to perform certain tasks (e.g. vulnerability assessment, penetration testing, threat modelling, programming cryptographic algorithms and conducting security reviews) and use essential industrial tools (e.g. kali Linux, Metasploit framework and ISO 27001 risk management framework) in the area of information security.

Pre-requisites if any: STAT – 115**:** Probability and Statistics and COMP -311**:** Computer Networks
Mode of Instruction: (Asynchronous/Synchronous): The mode of instructions will be synchronous in this course. However, the instructor can choose components of an asynchronous mode where necessary or according to the needs of the students.

Main Mode of Instruction: In the blended model of learning, the mode of instructions will be face to face in the classroom and course material e.g. books, lecture slides, lecture notes, video tutorials, any other tutorials or instructions and recorded lectures (where necessary) will be available on the Moodle. However, all the course material, instructions and announcements will be shared through the Moodle.

In the online model of learning, the mode of instructions will be live classroom sessions on the Google Meet and course material e.g. books, lecture slides, lecture notes, video tutorials, any other tutorials or instructions and recorded lectures (where necessary) will be available on Moodle. However, all the course material, instructions and announcements will be shared through the Moodle.

Considerations for Students with Limited Internet/Technology Access: The course material e.g. books, lectures slides, lecture notes; video tutorials, any other tutorials or instructions and recorded lectures (where necessary) will be available on Moodle.

Program Objectives Addressed:

A. Effectively apply knowledge and skills of computing to the real world problems.
B. Work collaboratively in teams and demonstrate appropriate leadership.

Course Objectives / Student Learning Outcomes (SLOs)

1. This course severs the purpose of providing basic knowledge to students relevant to the field of information security. The course also introduces the various sub-disciplines under the umbrella of information security e.g. software / program security, data security, network security, access control and organizational security.

2. After taking this course, the students should be able to choose a further field of study if they want to pursue education or should be able to secure an entry level / internship position in the industry relevant to information security.

3. After taking this course, the students will have some awareness of basic tools, techniques and security controls to protect the software systems / networks from the potential harms caused by the attackers.

Course Content, Learning Material & Activities Schedule

The schedule is tentative because it is not possible to anticipate exactly how much time each topic will require.

WK	Topic/ Title	Teaching-Learning Activities	Assessment
1	Introduction to the course and installation of	Lectures.	Will help in doing and

	Kali Linux and Git for submitting course deliverables.	A discussion session. Practical demonstration / Tutorial sessions.	submitting assignments.
2	Introduction to information security. • Information security definitions and basics. • Security principles / goals e.g. confidentiality, integrity and availability (CIA). • Security vulnerabilities, threats and controls.	Lectures.	Quiz 1 and Midterm exam.
3	Introduction to application security, vulnerability assessment and management. • What is application security, vulnerability assessment and management? • Types of vulnerability assessment e.g. active and passive, Host-based, etc. • Five stages of vulnerability management. • Difference between CVE and CWE.	Lectures. A discussion session.	Quiz 2 and Midterm exam.
4	Introduction to penetration testing. • What is penetration testing? • Vulnerability assessment versus penetration testing • Black, white and grey-box penetration testing techniques.	Lectures. Discussion / tutorial sessions.	Midterm exam.
5	Penetration testing methodology / phases. • Reconnaissance. • Scanning. • Vulnerability Assessment. • Exploitation. • Reporting. • Read, blue and purple testing teams.	Lectures. Discussion / tutorial sessions.	Midterm exam.
6	Using Metasploit framework to perform penetration testing. • Installing and configuring Metasploit within Kali Linux. • Installing Metasploitable-2 machine. • Installing and configuring other tools like Burpsuite and Nikto and any other relevant tools. • Demo of using Metasploit commands to exploit a known vulnerability. • Demo for performing a SQL Injection attack.	Practical demonstration / tutorial sessions. A discussion session.	Allocation of Assignment 1.
7	Introduction to cryptography and data security. • Symmetric and Asymmetric encryption techniques. • Advanced Encryption Standard (AES) Algorithm. • Rivest, Shamir, Adleman (RSA)	Lectures. A discussion session.	Midterm exam.

	Algorithm.		
8	Introduction to cryptography and data security. • The application of RSA algorithm such as digital signatures. • Introduction to cryptographic protocols e.g. Transport Layer Security (TLS) and Secure Shell Protocol (SSH). • The concept and usage of hashing and hashing algorithms.	Lectures. Discussion / tutorial sessions.	Submission of Assignment 1.
Midterm Exam			
9	Introduction to cryptography and data security. • Introduction to cloud security and the shared responsibility model for cloud security. • What is cloud security posture management? • Introduction to AWS security.	Lectures. Discussion / tutorial sessions.	Quiz 3. Allocation of Assignment 2.
10	Introduction to the DevSecOps. • What is DevSecOps? • Getting started with DevSecOps. • DevSecOps core and additional practices. • How to implement DevSecOps as a course project.	Lectures. Discussion / tutorial sessions.	Final exam. Allocation of Course Project.
11	Introduction to Identity and Access Management (IAM). • What is Access Control and IAM? • What is authentication and authorization? • Authorization techniques such as Role Based Access Control (RBAC). • Using Open Authorization (OAuth) • Using Auth0 authentication service for your applications.	Lectures. Discussion / tutorial sessions.	Quiz 4 and Final exam. Submission of Assignment 2.
12	Implementing Information Security Management System using ISO 27001 Framework. • What is Information Security Management System (ISMS)? • What is ISO 27001 framework? • Eleven Clauses of the ISO 27001 framework. • What is risk assessment and management and how to conduct risk assessment and management using ISO 27001 framework.	Lectures. Discussion / tutorial sessions.	Quiz 4 and Final exam.
13	Implementing Information Security Management System using ISO 27001 Framework. • Annex A for the ISO 27001 framework to understand the security controls.	Lectures. Class Activity. A discussion session.	Final exam.

	- A case study of Implementing ISO 27001 framework in small and medium enterprises.		
14	Introduction to Network Security. - What is network security and security at the OSI reference / TCP /IP model? - What is a firewall and a DMZ network? - Types of firewalls. - Introduction to intrusion detection and prevention systems.	Lectures. Discussion / tutorial sessions.	Final exam. Course Project Submission.
15	Introduction to Network Security. - How to conduct penetration testing at the network level. - An introduction to the Network Mapper (NMAP) and its graphical version (ZENMAP) tools. - Introduction on using PFsense open source firewall.		Final exam. Allocation of Assignment 3. Course Project Viva.
16	Final Exam & Submission of Assignment 3.		

Textbooks and Reference-books

Course text book covering all aspect of the course: Michael E. Whitman and Herbert J. Mattord (2021), Principles of Information Security, 7th edition, Cengage Learning, ISBN-13: 978-0357506561. (Available online to purchase).
Course text book covering all aspect of the course: Charles P. Pfleeger and Shari Lawrence Pfleeger (2015), Security in computing, 5th edition, Prentice Hall, ISBN-13: 978-0132390774. (PDF copy is available on Moodle).
Course text book covers the cryptography and data security part of the course: Christof Paar and Jan Pelzl (2009), Understanding cryptography: A textbook for students and practitioners, 1st edition, Springer Publishing Company, ISBN: 3642041000 9783642041006. (PDF copy is available on Moodle).
Reference book covering all aspects of the course: Ross J. Anderson (2020), Security Engineering: a guide to building dependable distributed systems, 3rd Edition, Wiley Publications. (Available through the web page: https://www.cl.cam.ac.uk/~rja14/book.html).
Reference book covering software security part of the course: John Viega and Gary McGraw (2011), Building secure software: How to avoid security problems the right way, Addison-Wesley Professional Computing Series, 1st edition, ISBN-13: 978-0321774958. (Available online to purchase).
Reference book covering cryptography part of the course: Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Wiley, ISBN-13: 978-0471117094. (Available online to purchase).

Course Requirements:

In this section, the information about each graded component is provided.

Class Participation / Attendance:

The attendance of live course lectures / presentation and class discussions is compulsory. The class participation will help students for better learning and help students to prepare for the course grading components e.g. as quizzes, assignments, exams and the course project.

Assignment 1:

In the assignment 1, you will be asked to perform a SQL injection attack. The reading materials / tutorials to do this assignment will be shared with you. The description of assignment 1 will be shared with you after the introduction of the SQL Injection topic.

Assignment 2:

In the assignment 2, you will be asked to implement a RSA Algorithm as an application of data security. The reading materials / tutorials to do this assignment will be shared with you. The description of assignment 2 will be shared with you after the introduction of the cryptography and RSA algorithm.

Assignment 3:

In the assignment 3, you will be asked to install and configure the firewalls using PFsense tool and to using Network Mapper (Nmap) for analyzing the traffic data. The reading materials / tutorials to do this assignment will be shared with you. The description of assignment 3 will be shared with you after the introduction of network security and firewalls.

Assignment Due Dates:

All assignments should be submitted till 11:59 pm on the due date. The due dates will be communicated beforehand after the introduction of the topic of assignment.

Test and Quizzes

I will take **four (4) quizzes** in this course as indicated in the lesson plan. In addition to the quizzes, I will take a **midterm exam** and a **final exam** in this course. **There will be no retake of any quiz and exam.**

Course Project

There will be a course project as a grading component of this course. You will do the course project into the group of three people. In your course project, you are required to implement the DevSecOps cycle using DevOps tool and configuring these tools with security testing tools. More details about the course project will be shared with you after the introduction of DevSecOps.

The breakup is as follows:

Class Attendance	5%
Assignments:	20%
Quizzes:	15%
Midterm exam:	20%
Final term exam:	25%
Course project:	15%
TOTAL:	100%

Missed Assignments/ Make-Ups/ Extra Credit

In this course, there will be no retakes for any missed quizzes, exams, assignments and course project. In case of late submission of any deliverable e.g. assignments and course project, the instructor will deduct ten percent (10%) marks per day from the obtained marks of the student.

Attendance Policy:

Your class attendance is compulsory. The five percent (5%) of your grading component is allocated to attendance which is indicated in the course requirements' section.

.

Classroom Participation:

As a teacher, I not only deliver lectures and provide explanation of concepts and demonstration of technique but also give importance to interactive learning. Therefore, I encourage all students to actively participation in the class discussions and ask questions when they do not understand any concept or part of the lecture. The students are allowed to ask questions any time during the lecture.

Grade Determination & Course Assessment as per FCC Policy:

In this course, I have adopted a **relative grading policy** consistent with the department of computer science and FCC. However, I should mention that the performance of class in terms of **average and standard deviation** will determine the class grades. There should be no confusion on this. In case of late submission of any deliverable e.g. assignments and course project, the instructor will deduct ten percent (10%) marks per day from the obtained marks of the student.

Student Conduct & Other Issues:

- As an instructor, I expect that all the students will use proper language / do not use offensive words / comments and behave according to the norms and to the core values of the FCC during class discussions and classroom lectures. It is also expected that each student will follow the civil norms and will treat the other students and the instructor respectfully.

- If any student faces any issues or has any concerns regarding the classroom climate and interactions, please feel free to contact VR office ___ gloriacalib@fccollege.edu.pk

Changes to the Syllabus:

This syllabus was designed to convey course information and requirements as accurately as possible. It is important to note however that it **may** be subject to change during the course depending on the needs of the class and other situational factors. Such changes would be for your benefit and you will be notified of them as soon as possible.

Student Support Services

- Student Counseling Services. The students can contact the Campus Counseling Center at 0331-444-1518 or email ccc@fccollege.edu.pk.
- Writing Center
- Mercy Health Center

Other Useful FCCU Policy Documents:

- Sexual Harassment Policy
- Anti-Corruption Policy
- Academic integrity
- Plagiarism Policy
- Academic Calendar

Honor FCC Core Values and Academic Honesty:

- I expect that you will strictly follow the core values of FCCU and put your entire efforts to learn as per the course requirements, attend classes, read the textbook(s)/other assigned reading material and do the assignments in the stipulated time period.
- All work that you submit in this course must be your own.
- Unauthorized group efforts are considered academic dishonesty.
- You may discuss homework (Assignments, Course Project) in a general way with others, but you may not consult anyone else's written work.
- You are guilty of academic dishonesty if you examine another's solution, allows (actively or passively) another student to examine your solution, or you copy from the Internet without complete understanding of what you have done. University policy of plagiarism will be applicable in the case.
- All cases no matter how trivial they are can be reported to Academic Integrity Committee (AIC) of FCCU.
- Cheating or violation of academic integrity in any exam will cause a fail (F) grade.

https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-documentation.pdf